European Court of Human Rights Confirms: Weakening Encryption Violates Fundamental Rights

Christoph Schmon ⋮ 8-10 minutes ⋮ 3/5/2024

In a milestone judgment—Podchasov v. Russia—the European Court of Human Rights (ECtHR) has ruled that weakening of encryption can lead to general and indiscriminate surveillance of the communications of *all* users and violates the human right to privacy.

In 2017, the landscape of digital communication in Russia faced a pivotal moment when the government required Telegram Messenger LLP and other “internet communication” providers to store all communication data—and content—for specified durations. These providers were also required to supply law enforcement authorities with users’ data, the content of their communications, as well as any information necessary to decrypt user messages. The FSB (the Russian Federal Security Service) subsequently ordered Telegram to assist in decrypting the communications of specific users suspected of engaging in terrorism-related activities.

Telegram opposed this order on the grounds that it would create a backdoor that would undermine encryption for all of its users. As a result, Russian courts fined Telegram and ordered the blocking of its app within the country. The controversy extended beyond Telegram, drawing in numerous users who contested the disclosure orders in Russian courts. A Russian citizen, Mr Podchasov, escalated the issue to the European Court of Human Rights (ECtHR), arguing that forced decryption of user communication would infringe on the right to private life under Article 8 of the European Convention of Human Rights (ECHR), which reads as follows:

> *Everyone has the right to respect for his private and family life, his home and his correspondence* (Article 8 ECHR, right to respect for private and family life, home and correspondence)

EFF has always stood against government intrusion into the private lives of users and advocated for strong privacy guarantees, including the right to confidential communication. Encryption not only safeguards users’ privacy but also protects their right to freedom of expression protected under international human rights law.

In a great victory for privacy advocates, the ECtHR agreed. The Court found that the requirement of continuous, blanket storage of private user data interferes with the right to privacy under the Convention, emphasizing that the possibility for national authorities to access these data is a crucial factor for determining a human rights violation [at 53]. The Court identified the inherent risks of arbitrary government action in secret surveillance in the present case and found again—following its stance in *Roman Zakharov v. Russia*—that the relevant legislation failed to live up to the quality of law standards and lacked the adequate and effective safeguards against misuse [75]. Turning to a potential justification for such interference, the ECtHR emphasized the need of a careful balancing test that considers the use of modern data storage and processing technologies and weighs the potential benefits against important private-life interests [62-64].

In addressing the State mandate for service providers to submit decryption keys to security services, the court's deliberations culminated in the following key findings [76-80]:

1. **Encryption being important for protecting the right to private life and other fundamental rights, such as freedom of expression:** The ECtHR emphasized the importance of encryption technologies for safeguarding the privacy of online communications. Encryption safeguards and protects the right to private life generally while also supporting the exercise of other fundamental rights, such as freedom of expression.
2. **Encryption as a shield against abuses:** The Court emphasized the role of encryption to provide a robust defense against unlawful access and generally “appears to help citizens and businesses to defend themselves against abuses of information technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information.” The Court held that this must be given due consideration when assessing measures which could weaken encryption.
3. **Decryption of communications orders weakens the encryption for all users:** The ECtHR established that the need to decrypt Telegram's "secret chats" requires the weakening of encryption for all users. Taking note again of the dangers of restricting encryption described by many experts in the field, the Court held that backdoors could be exploited by criminal networks and would seriously compromise the security of all users’ electronic communications.
4. **Alternatives to decryption:** The ECtHR took note of a range of alternative solutions to compelled decryption that would not weaken the protective mechanisms, such as forensics on seized devices and better-resourced

policing.

In light of these findings, the Court held that the mandate to decrypt end-to-end encrypted communications risks weakening the encryption mechanism for all users, which was a disproportionate to the legitimate aims pursued.

In summary [80], the Court concluded that the retention and unrestricted state access to internet communication data, coupled with decryption requirements, cannot be regarded as necessary in a democratic society, and are thus unlawful. It emphasized that a direct access of authorities to user data on a generalized basis and without sufficient safeguards impairs the very essence of the right to private life under the Convention. The Court also highlighted briefs filed by the European Information Society Institute (EISI) and Privacy International, which provided insight into the workings of end-to-end encryption and explained why mandated backdoors represent an illegal and disproportionate measure.

Impact of the ECtHR ruling on current policy developments

The ruling is a landmark judgment, which will likely draw new normative lines about human rights standards for private and confidential communication. We are currently supporting Telegram in its parallel complaint to the ECtHR, contending that blocking its app infringes upon fundamental rights. As part of a collaborative efforts of international human rights and media freedom organisations, we have submitted a third-party intervention to the ECtHR, arguing that blocking an entire app is a serious and disproportionate restriction on freedom of expression. That case is still pending.

The Podchasov ruling also directly challenges ongoing efforts in Europe to weaken encryption to allow access and scanning of our private messages and pictures.

For example, the controversial UK's Online Safety Act creates the risk that online platforms will use software to search all users' photos, files, and messages, scanning for illegal content. We recently submitted comments to the relevant UK regulator (Ofcom) to avoid any weakening of encryption when this law becomes operational.

In the EU, we are concerned about the European Commission's message-scanning proposal (CSAR) as being a disaster for online privacy. It would allow EU authorities to compel online services to scan users' private messages and compare users' photos to against law enforcement databases or use error-prone AI algorithms to detect criminal behavior. Such detection measures will inevitably lead to dangerous and unreliable Client-Side Scanning practices, undermining the essence of end-to-end encryption. As the ECtHR deems general user scanning as disproportionate, specifically criticizing measures that weaken existing privacy standards, forcing platforms like WhatsApp or Signal to weaken security by inserting a vulnerability into all users' devices to enable message scanning must be considered unlawful.

The EU regulation proposal is likely to be followed by other proposals to grant law enforcement access to encrypted data and communications. An EU high level expert group on 'access to data for effective law enforcement' is expected to make policy recommendations to the next EU Commission in mid-2024.

We call on lawmakers to take the Court of Human Rights ruling seriously: blanket and indiscriminate scanning of user communication and the general weakening of encryption for users is unacceptable and unlawful.

Join EFF Lists